UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,560	09/12/2003	Takanori Masui	117046	6405

25944   7590   03/27/2008
OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

EXAMINER
PAN, JOSEPH T

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
03/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 December 2007</u>.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-3 and 6-10</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-3 and 6-10</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>12 September 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☒ All   b)☐ Some * c)☐ None of:
        1.☒ Certified copies of the priority documents have been received.
        2.☐ Certified copies of the priority documents have been received in Application No. _____.
        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.　　A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection.　Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.　Applicant's submission filed on December 21, 2007 has been entered.

2.　　Applicant's response filed on December 21, 2007 has been carefully considered.　Claims 1-3 and 6-10 have been amended.　Claims 4, 5 and 11 have been canceled.　Claims 1-3, 6-10 are pending.

Claim Rejections - 35 USC § 103

3.　　The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.　Patentability shall not be negatived by the manner in which the invention was made.

4.　　Claims 1-3, 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Foster et al. (U.S. Pub. No. 2002/0184518 A1), hereinafter "Foster", in view of Sutton et al. (U.S. Patent No. 7,237,243 B2), hereinafter "Sutton".

Referring to claims 1, 7:

　　i.　　Foster teaches:

　　　　An information processor which implements a service by cooperatively operating at least first and second job processors, the first job processor to execute a first job processing in accordance with a first process description define din instruction data, the second job processor to execute a second job processing, which is a different type of processing from the first processing, in accordance with a

second process description defined in the instruction data including the first process description, the information processor comprising:

an encryption processor which encrypts the first and second process *description defined* in the instruction data (see figure 3, processors 80; figure 15, element 610 'encrypt job ticket'; and page 12, paragraph [0125] "The information in the job ticket 61 (excluding the public key signature field 67) is then, for example, optionally hashed using, for example, MD5 protocol, and encrypted with a public key encryption system, block 610, generating a hash number, block 615.   Other hashing or encryption techniques may also be used." of Foster, emphasis added), and

a transmitter which sends the instruction data, in which the first and second process descriptions are encrypted by the encryption processor, to at least one of the first and second job processors (see page 10, paragraph [0108] "Access may be controlled [i.e., by job ticket service] by a password, an identification, and a public key/private key security system, for example", of Foster).

Foster discloses encrypting the process description (see e.g. figure 15, element 610 'encrypt job ticket', of Foster).   However, Foster does not specifically mention encrypting each process description using the information of each one of job processor which executes the process.

ii.   Sutton teaches a multiple device management method wherein Sutton discloses encrypting each process description using the information of each one of job processor which executes the process (see column 12, lines 19-23, 'Since rogue computers can also sniff the network, sensitive information is not passed over the network unencrypted, and the encryption is such that only the target nodes of a secured message can decrypt it.', of Sutton, emphasis added).

iii.   It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sutton into the method of Foster to encrypt each process description using the information of each one of job processor which executes the process.

iv.   The ordinary skilled person would have been motivated to have applied the teaching of Sutton into the system of Foster to encrypt each process description using the information of each one of job processor which executes the process, because "Since rogue computers can also sniff the network" (see column 12, lines 19-23 of Sutton), the data security will be enhanced by encrypting each process description using the information of each one of job processor which executes the process.

Referring to claim 2:

Foster and Sutton teach the claimed subject matter: an information processor which implements a service by cooperatively operating at least first and second job processors (see claim 1 above). Foster further discloses the encrypting the process description (see page 11, paragraph [0125], "The information in the job ticket 61 (excluding the public key signature field 67) is then, for example, optionally hashed using, for example, MD5 protocol, and **encrypted** with a public key encryption system, block 610, generating a hash number, block 615.", of Foster, emphasis added).

Referring to claim 3:

Foster and Sutton teach the claimed subject matter: an information processor which implements a service by cooperatively operating at least first and second job processors (see claim 1 above). Foster further discloses encrypting the process description with the public key (see page 11, paragraph [0125], "The information in the job ticket 61 (excluding the public key signature field 67) is then, for example, optionally hashed using, for example, MD5 protocol, and encrypted with **a public key encryption system**, block 610, generating a hash number, block 615.", of Foster, emphasis added).

Referring to claims 6, 8, 10:

i.   Foster teaches:

An information processor contained in a system which implements a service through cooperative operation of a plurality of job processors, the information processor comprising:

a receiver which receives instruction data, the instruction data including a first process description representing a first processing to be processed by a first job processor and a second process description representing a second processing to be processed by a second job processor (see page 6, paragraph [0064] of Foster);

a decryption processor which decrypts the first process decryption in the instruction data received by the receiver (see page 6, paragraph [0064] of Foster);

a processing section that executes the first processing in accordance with the decrypted first process description (see page 6, paragraph [0064] of Foster);

a transmitter which sends the instruction data to the second job processor which, subsequently executes the second processing (see page 6, paragraph [0064] of Foster).

Foster discloses encrypting the process description (see e.g. figure 15, element 610 'encrypt job ticket', of Foster). However, Foster does not specifically mention encrypting each process

description using the information of each one of job processor which executes the process. Neither does Foster specifically mention deleting the part of the process description from the instruction data.

        ii.   Sutton teaches a multiple device management method wherein Sutton discloses encrypting each process description using the information of each one of job processor which executes the process (see column 12, lines 19-23, 'Since rogue computers can also sniff the network, sensitive information is not passed over the network unencrypted, <u>and the encryption is such that only the target nodes of a secured message can decrypt it</u>.', of Sutton, emphasis added).

        Sutton further discloses deleting the part of the process description from the instruction data (see column 8, lines 52-58 'The administration program 210 or the like enables the creation or editing of a script on the file-system, creation of a script entry in the script database, <u>editing of a script entry</u>, <u>deletion of a script entry</u>, creation of a job (described below) that may use a script, deletion of a job, editing of a job, execution of a job, a retrieval of the status and results of a job.', of Sutton, emphasis added).

        iii.   It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sutton into the method of Foster to encrypt each process description using the information of each one of job processor which executes the process.

        It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sutton into the method of Foster to be able to edit or delete the part of the process description from the instruction data.

        iv.   The ordinary skilled person would have been motivated to have applied the teaching of Sutton into the system of Foster to encrypt each process description using the information of each one of job processor which executes the process, because "Since rogue computers can also sniff the network" (see column 12, lines 19-23 of Sutton), the data security will be enhanced by encrypting each process description using the information of each one of job processor which executes the process.

        The ordinary skilled person would have been motivated to have applied the teaching of Sutton into the system of Foster to be able to edit or delete the part of the process description from the instruction data, because "This feature may eliminate stale data, and free up resources for another job requests" (see page 8, paragraph [0085] of Foster).

    <u>Referring to claim 9</u>:

        i.   Foster teaches:

A job processor which carries out a job according to a process description defined in instruction data, the job processor comprising:

an encryption processor which encrypts each subsequent first and second process descriptions defined in the instruction data using information of each one of job processor which executes the process, for at least one of a first job processor and a second job processor, the first job processor to execute a first job processing in accordance with a first process description defined in the instruction data, and the second job processor to execute a second processing, which is a different type of processing from the first processing, in accordance with the second process description defined in the instruction data including the first process description (see figure 3, processors 80; figure 15, element 610 'encrypt job ticket'; and page 12, paragraph [0125] "The information in the job ticket 61 (excluding the public key signature field 67) is then, for example, optionally hashed using, for example, MD5 protocol, and encrypted with a public key encryption system, block 610, generating a hash number, block 615. Other hashing or encryption techniques may also be used." of Foster, emphasis added), and

a transmitter which sends the instruction data, in which the first and second process descriptions are encrypted by the encryption processor, to at least one of the first and second job processors (see page 6, paragraph [0064] of Foster).

Foster discloses encrypting the process description (see e.g. figure 15, element 610 'encrypt job ticket', of Foster). However, Foster does not specifically mention encrypting each process description using the information of each one of job processor which executes the process.

ii.   Sutton teaches a multiple device management method wherein Sutton discloses encrypting each process description using the information of each one of job processor which executes the process (see column 12, lines 19-23, 'Since rogue computers can also sniff the network, sensitive information is not passed over the network unencrypted, and the encryption is such that only the target nodes of a secured message can decrypt it.', of Sutton, emphasis added).

iii.   It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Sutton into the method of Foster to encrypt each process description using the information of each one of job processor which executes the process.

iv.   The ordinary skilled person would have been motivated to have applied the teaching of Sutton into the system of Foster to encrypt each process description using the information of each one of job processor which executes the process, because "Since rogue computers can also sniff the network"

(see column 12, lines 19-23 of Sutton), the data security will be enhanced by encrypting each process description using the information of each one of job processor which executes the process.

Response to Arguments

5.   Applicant's arguments, filed on December 21, 2007, have been fully considered but they are not persuasive.

Applicant argues:

"Applicants maintain previously asserted positions that (1) the Office Action unreasonably interprets Foster for what it can be considered to teach, or to have suggested, with respect to the subject matter of the pending claims; (2) Applicants' previous arguments in this regard are not addressed in the current Office Action; (3) the asserted combination of Foster and Sutton is unreasonable; (4) it is unclear how the Office Action actually proposes that the teaching of Foster can be modified by any teaching of Sutton; and (5) the Office Action fails to establish a prima facie case for obviousness of the subject matter of the pending claims over the applied references." (see page 2, 2nd paragraph, Applicant's Arguments/Remarks, emphasis added)

Examiner maintains:

For Applicant's asserted positions of (1), (2), (5):

Claims 1-3, 6-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Foster in view of Sutton.

For example, Foster discloses encrypting the process description (see e.g. figure 15, element 610 'encrypt job ticket', of Foster). However, Foster does not specifically mention encrypting each process description using the information of each one of job processor which executes the process. On the other hand, Sutton teaches a multiple device management method wherein Sutton discloses encrypting each process description using the information of each one of job processor which executes the process (see e.g. Office Action for claim 1 above).

Therefore, the combination of Foster and Sutton discloses the claimed invention such as described in the Claim 1.

For Applicant's asserted positions of (3), (4):

Foster discloses "These and other problems are solved by a method and an apparatus that controls access to a job ticket and associated content through use of a job ticket service. The job ticket

service includes mechanisms that arbitrate access to the job ticket among multiple users of the job ticket, limit access to the job ticket by incorporating **security features**, and ensure modifications made by one processor or user are reflected in the job ticket and the content." (see page 2, paragraph [0035], lines 1-8 of Foster, emphasis added).

Foster further discloses "The job ticket 61 may be signed with an industry standard public key encryption message digest (MD) signature, and may be protected by a public key encryption system." (see page 6, paragraph [0064], lines 1-4 of Foster, emphasis added).

Therefore, Foster discloses limit access to the job ticket by incorporating security features, such as encrypting a job ticket [i.e., job description] (see figure 15, element 610 'encrypt job ticket' of Foster).

On the other hand, Sutton discloses "Since rogue computers can also sniff the network, sensitive information is not passed over the network unencrypted, and the encryption is such that only the target nodes of a secured message can decrypt it." (see column 12, lines 19-23 of Sutton).

Therefore, Sutton's teaching could enhance Foster's system to encrypt a job ticket [i.e., job description] specific to target nodes.

Conclusion

6.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan

March 14, 2008

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135